

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-150554

(43)公開日 平成11年(1999)6月2日

| (51)Int.Cl.* | 識別記号  | F I          |         |
|--------------|-------|--------------|---------|
| H 04 L 12/54 |       | H 04 L 11/20 | 1 0 1 B |
|              | 12/58 | G 06 F 13/00 | 3 5 1 Z |
| G 06 F 13/00 | 3 5 1 | H 04 L 9/00  | 6 7 3 A |
| H 04 L 9/32  |       |              |         |

審査請求 未請求 請求項の数16 O.L (全16頁)

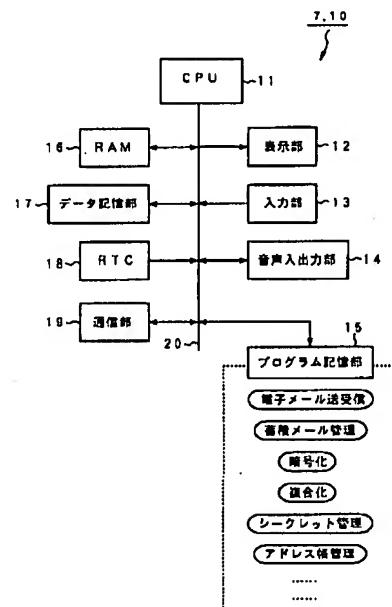
|          |                  |         |  |
|----------|------------------|---------|--|
| (21)出願番号 | 特願平9-313671      | (71)出願人 | 000001443<br>カシオ計算機株式会社<br>東京都渋谷区本町1丁目6番2号       |
| (22)出願日  | 平成9年(1997)11月14日 | (72)発明者 | 遠藤 典夫<br>東京都羽村市栄町3丁目2番1号 カシオ<br>計算機株式会社羽村技術センター内 |
|          |                  | (74)代理人 | 弁理士 荒船 博司 (外1名)                                  |
|          |                  |         |  |

(54)【発明の名称】 データ通信装置、データ通信方法及び記憶媒体

(57)【要約】

【課題】 データ通信において、通常は暗号化を行わずに、機密保持が必要な場合にのみデータの暗号化を行うことによって、不要な操作を減らし、且つ、機密を保持することが可能なデータ通信装置、データ通信方法及び記憶媒体を提供する。

【解決手段】 通信手段を介して接続された外部機器との間でデータを送受信するデータ通信装置において、データを送信する送信手段と、この送信手段によってデータを送信することが可能な宛先を記憶する宛先記憶手段と、この宛先記憶手段に記憶された各宛先毎に、送信されるデータを暗号化するか否かを指示する暗号化指示データを記憶する暗号化指示データ記憶手段と、この暗号化指示データ記憶手段に記憶された暗号化指示データによって暗号化すべきと指定された宛先に、送信手段によってデータが送信される場合には、該データを暗号化して送信手段に送信させる暗号化手段と、を備えるデータ通信装置。



1

## 【特許請求の範囲】

【請求項1】通信手段を介して接続され、他の通信機器にデータを送信するデータ通信装置において、送信するデータ毎に暗号化するか否かを記憶した暗号化指示データ記憶手段と、この暗号化指示データ記憶手段に記憶した暗号化の正否に基づいて前記データの暗号化を制御する暗号化手段と、この暗号化手段の制御により暗号化あるいは非暗号化されたデータを送信する送信手段と、を備えたことを特徴とするデータ通信装置。

【請求項2】前記暗号化指示データ記憶手段は、送信するデータの宛先毎に、送信するデータを暗号化するか否かを指示する暗号化データを記憶することを特徴とする請求項1記載のデータ通信装置。

【請求項3】前記暗号化指示データ記憶手段は、前記データを暗号化するキーワードを記憶しており、前記暗号化手段は、前記データがこの暗号化指示データ記憶手段に記憶されたキーワードを含んでいると該データを暗号化することを特徴とする請求項1記載のデータ通信装置。

【請求項4】前記送信手段は、前記暗号化あるいは非暗号化されたデータとともにキーワードを送信することを特徴とする請求項3記載のデータ通信装置。

【請求項5】前記暗号化指示データ記憶手段は、前記記憶されている暗号化指示データ毎あるいはキーワード毎に異なる暗号化キーあるいは異なる暗号化方式を記憶し、前記暗号化手段は、この暗号化指示データ記憶手段に記憶された暗号化キーあるいは暗号化方式に基づいて暗号化することを特徴とする請求項2、3または4記載のデータ通信装置。

【請求項6】通信手段を介して接続され、他の通信機器からデータを受信するデータ通信装置において、前記受信するデータ毎に暗号化されたデータかを記憶する暗号化データ記憶手段と、この暗号化データ記憶手段に記憶した暗号化の正否に基づいて前記データの復号化を指示する復号化指示データを記憶する復号化指示データ記憶手段と、この復号化指示データ記憶手段に基づいて復号化を制御する復号化手段と、この復号化手段の制御により復号化あるいは非復号化されたデータを表示する表示手段と、を備えたことを特徴とするデータ通信装置。

【請求項7】前記復号化指示データ記憶手段は、受信するデータの送信先毎にデータを復号化するか否かを指示する復号化指示データを記憶することを特徴とする請求項6記載のデータ通信装置。

【請求項8】前記復号化指示データ記憶手段は、前記データを復号化するキーワードを記憶しており、

2

前記復号化手段は、この復号化指示データ記憶手段に記憶されているキーワードに基づいて前記データを復号化することを特徴とする請求項6記載のデータ通信装置。

【請求項9】前記復号化手段は、前記復号化指示データ記憶手段にキーワードが記憶されていると前記データを復号化することを特徴とする請求項8記載のデータ通信装置。

【請求項10】前記暗号化あるいは非暗号化されたデータと共にキーワードを受信し、前記復号化手段は、受信したキーワードが前記復号化指示データ記憶手段に記憶されていると前記データを復号化することを特徴とする請求項8記載のデータ通信装置。

【請求項11】前記復号化指示データ記憶手段は、前記記憶されている復号化指示データ毎あるいはキーワード毎に異なる復号化キーあるいは異なる復号化方式を記憶し、

前記復号化手段は、この復号化指示データ記憶手段に記憶された復号化キーあるいは復号化方式に基づいて復号化することを特徴とする請求項6、7、8、9または10記載のデータ通信装置。

【請求項12】通信手段を介して接続された外部の通信機器との間でデータ通信を行うデータ通信装置を利用したデータ通信方法において、データを送受信することが可能な外部の通信機器を送受信先として記憶し、これらの各送受信先が、該送受信先との間のデータ通信を秘密化すべき秘密通信先か否かをそれぞれ指定する秘密指定データを記憶し、この秘密指定データによって秘密通信先と指定された前記送受信先に対してデータを送信する際には、該データを暗号化して送信し、

前記秘密指定データによって秘密通信先と指定された前記送受信先から送信されたデータを受信した際には、該データを秘密データとして記憶し、

前記秘密指定データによって秘密通信先と指定されない前記送受信先から送信されたデータを受信した際には、該データを通常データとして記憶すること、を特徴とするデータ通信方法。

【請求項13】通信手段を介して接続された外部の通信機器との間においてデータ通信を行うデータ通信装置を利用したデータ通信方法において、

予め任意に設定される鍵情報を記憶し、前記データ通信機器によって送受信されるデータの内容に、前記鍵情報記憶手段に記憶された鍵情報が含まれているか否かを検知し、

前記データ通信装置によって前記データを送信する際に、該データの内容に前記鍵情報が検知された場合には、該データを暗号化して送信し、

前記データ通信装置が前記データを受信した際に、該データの内容に前記鍵情報が検知された場合には、該データを秘密データとして記憶し、

前記データ通信装置が前記データを受信した際に、該データの内容に前記鍵情報が検知されない場合には、該データを通常データとして記憶すること、を特徴とするデータ通信方法。

【請求項14】通信手段を介して接続された外部の通信機器との間でデータ通信を行うためのコンピュータが読み取り可能なプログラムを格納した記憶媒体であって、データを送信するためのプログラムコードと、データを送信することが可能な他のデータ通信装置を送受信先と、該送信先との間のデータ通信を秘密化すべき秘密通信先か否かをそれぞれ指定する秘密指定データを記憶するためのプログラムコードと、この秘密指定データによって秘密通信先と指定された前記送信先に対してデータを送信する際に、該データを暗号化して送信するためのプログラムコードと、を格納したことと特徴とする記憶媒体。

【請求項15】通信手段を介して接続された外部の通信機器との間においてデータ通信を行うためのコンピュータが読み取り可能なプログラムを格納した記憶媒体であって、データを送受信するためのプログラムコードと、任意に設定される鍵情報を記憶するためのプログラムコードと、送受信されるデータの内容に、前記鍵情報記憶手段に記憶された鍵情報が含まれているか否かを検知するためのプログラムコードと、前記送受信手段によってデータを送信するあるいはデータを受信した際に、該データの内容に前記鍵情報が検知された場合には、該データを暗号化して送信するあるいは該データを暗号化して記憶するためのプログラムコードと、を格納したことと特徴とする記憶媒体。

【請求項16】前記暗号化されたデータを受信すると秘密データとして記憶し、該暗号化されていないデータを受信すると通常データとして記憶するためのプログラムコードをさらに格納したことと特徴とする請求項15記載の記憶媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、電子メール等のデータ通信を行うためのデータ通信装置、データ通信方法及び記憶媒体に関する。

##### 【0002】

【従来の技術】近年、コンピュータネットワークの普及に伴って、電子メール等のデータ通信が広く行われるようになった。

【0003】一般に、データ通信は公衆回線や無線通信手段を介して行われることが多く、機密保持という点からいえば、必ずしも安全な環境ではない。このため、機密保持のために様々な手段が開発されてきた。

【0004】例えば、従来用いられている電子メール送受信用ソフトウェアとして、送信する電子メール自体を暗号化して送信するソフトウェアがある。このソフトウェアによって送信された電子メールを受信したユーザーは、電子メールを復号化した後に閲覧する。また、送信元のユーザーと共に通のパスワードをこと前に決めておき、このパスワードを入力することによって電子メールの復号化が可能になるというソフトウェアや、パスワードを入力しなければ電子メールの閲覧ができないようになっているソフトウェアが利用されてきた。

##### 【0005】

【発明が解決しようとする課題】ところが、上記のような方法で機密保持を行うと、暗号化する必要のない電子メールと暗号化すべき電子メールとを区別して送信することができず、特に暗号化する必要がない電子メールを送信したり、閲覧する場合にもパスワードを入力しなければならないという問題点があった。このため、操作が非常に煩雑になってしまふという問題があった。

【0006】この発明は、上記問題点を解決するため、データ通信において、通常は暗号化を行わずに、機密保持が必要な場合にのみデータの暗号化を行うことによって、不要な操作を減らし、且つ、機密を保持することが可能なデータ通信装置、データ通信方法及び記憶媒体を提供することである。

##### 【0007】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の発明は、通信手段を介して接続され、他の通信機器にデータを送信するデータ通信装置において、送信するデータ毎に暗号化するか否かを記憶した暗号化指示データ記憶手段と、この暗号化指示データ記憶手段に記憶した暗号化の正否に基づいて前記データの暗号化を制御する暗号化手段と、この暗号化手段の制御により暗号化あるいは非暗号化されたデータを送信する送信手段と、を備えたことを特徴とする構成とした。

【0008】この請求項1記載の発明のデータ通信装置によれば、通信手段を介して接続され、他の通信機器にデータを送信するデータ通信装置において、暗号化指示データ記憶手段により、送信するデータ毎に暗号化するか否かを記憶し、暗号化手段により、暗号化指示データ記憶手段に記憶した暗号化の正否に基づいてデータの暗号化を制御し、送信手段により、暗号化手段の制御により暗号化あるいは非暗号化されたデータを送信する。

【0009】これによって、予め暗号化指示データ記憶手段によって暗号化すべきデータを指定しておくことによって、データを送信する毎にデータの暗号化を指示する必要がなく、作業者の操作を減らすことが可能であり、さらに秘密を確実に保持することができる。

【0010】ここで、通信手段とは、例えば公衆回線網等の通信回線であっても良く、また、独立した専用線であっても良いし、有線または無線を問わずデータ通信を

仲介することができるものであればよい。

【0011】請求項2記載の発明は、請求項1記載のデータ通信装置であって、前記暗号化指示データ記憶手段は、送信するデータの宛先毎に、送信するデータを暗号化するか否かを指示する暗号化データを記憶することを特徴とする構成とした。

【0012】この請求項2記載の発明のデータ通信装置によれば、請求項1記載のデータ通信装置において、暗号化指示データ記憶手段は、送信するデータの宛先毎に、送信するデータを暗号化するか否かを指示する暗号化データを記憶する。

【0013】従って、例えばアドレス帳機能を有するデータベースに記載された各宛先に対して、それぞれ暗号化したデータを送信するか、あるいは通常のデータを送信するかを予め設定しておくことによって、データを通常通り送信しても、情報の秘匿が必要な相手へデータを送信する場合には自動的にデータが暗号化される。

【0014】請求項3記載の発明は、請求項1記載のデータ通信装置において、前記暗号化指示データ記憶手段は、前記データを暗号化するキーワードを記憶しており、前記暗号化手段は、前記データがこの暗号化指示データ記憶手段に記憶されたキーワードを含んでいると該データを暗号化することを特徴とする構成とした。

【0015】この請求項3記載の発明のデータ通信装置によれば、請求項1記載のデータ通信装置において、暗号化指示データ記憶手段は、データを暗号化するキーワードを記憶し、暗号化手段は、データがこの暗号化指示データ記憶手段に記憶されたキーワードを含んでいると該データを暗号化する。

【0016】これによって、予め設定されたキーワードを含むデータの暗号化が実行されるので、ある特定のテーマに関わるデータを全て暗号化したい場合などに、各データ毎に暗号化を設定しなくても、該テーマをキーワードに設定することによって暗号化を行うことができる。そして、各データについて設定を個々に行う場合に比べて、設定漏れ等のミスを減少させることができる。

【0017】請求項4記載の発明は、請求項3記載のデータ通信装置において、前記送信手段は、前記暗号化あるいは非暗号化されたデータとともにキーワードを送信することを特徴とする構成とした。

【0018】請求項4記載の発明のデータ通信装置によれば、請求項3記載のデータ通信装置において、送信手段は、暗号化あるいは非暗号化されたデータとともにキーワードを送信する。

【0019】これによって、請求項3記載のデータ通信装置においてデータを送信する際に、例えば、電子メールのタイトルのような形式によってキーワードがデータ本文に付されて送信されるので、データ本文を参照することなくキーワードを容易に認識することが可能となり、利便性をより高めることができる。

【0020】請求項5記載の発明は、請求項2、3または4記載のデータ通信装置において、前記暗号化指示データ記憶手段は、前記記憶されている暗号化指示データ毎あるいはキーワード毎に異なる暗号化キーあるいは異なる暗号化方式を記憶し、前記暗号化手段は、この暗号化指示データ記憶手段に記憶された暗号化キーあるいは暗号化方式に基づいて暗号化をすることを特徴とする構成とした。

【0021】この請求項5記載の発明のデータ通信装置によれば、請求項2、3または4記載のデータ通信装置において、暗号化指示データ記憶手段は、記憶されている暗号化指示データ毎あるいはキーワード毎に異なる暗号化キーあるいは異なる暗号化方式を記憶し、暗号化手段は、この暗号化指示データ記憶手段に記憶された暗号化キーあるいは暗号化方式に基づいて暗号化をする。

【0022】従って、暗号化指示データあるいはキーワードが異なるデータに対しては、暗号化キーあるいは暗号化方式が異なるので、他のデータに適用された暗号化キーあるいは暗号化方式を容易に流用することが困難になるので、より確実に秘密を保持することができる。

【0023】請求項6記載の発明は、通信手段を介して接続され、他の通信機器からデータを受信するデータ通信装置において、前記受信するデータ毎に暗号化されたデータかを記憶する暗号化データ記憶手段と、この暗号化データ記憶手段に記憶した暗号化の正否に基づいて前記データの復号化を指示する復号化指示データを記憶する復号化指示データ記憶手段と、この復号化指示データ記憶手段に基づいて復号化を制御する復号化手段と、この復号化手段の制御により復号化あるいは非復号化されたデータを表示する表示手段と、を備えたことを特徴とする構成とした。

【0024】この請求項6記載のデータ通信装置によれば、通信手段を介して接続され、他の通信機器からデータを受信するデータ通信装置において、暗号化データ記憶手段により、受信するデータ毎に暗号化されたデータかを記憶し、復号化指示データ記憶手段により、暗号化データ記憶手段に記憶した暗号化の正否に基づいて前記データの復号化を指示する復号化指示データを記憶し、復号化手段により、復号化指示データ記憶手段に記憶された復号化指示データに基づいて復号化を制御し、表示手段により、復号化手段の制御により復号化あるいは非復号化されたデータを表示する。

【0025】これによって、データ通信装置において受信したデータが暗号化されているか否かを予め設定することが可能であるので、暗号化されたデータを受信するとともに該データを復号化することができる。従って、データを受信して閲覧する毎に復号化を設定する必要がなく、作業者の操作を減らすことが可能である。

【0026】請求項7記載の発明は、請求項6記載のデータ通信装置であって、前記復号化指示データ手段は、

受信するデータの送信元毎に、データを復号化するか否かを指示する復号化指示データを記憶することを特徴とする構成とした。

【0027】この請求項7記載の発明のデータ通信装置によれば、請求項6記載のデータ通信装置において、復号化指示データ記憶手段は、受信するデータの送信元毎に、データを復号化するか否かを指示する復号化指示データを記憶する。

【0028】これによって、秘密を保持したいデータを送受信する相手先を予め登録しておくことによって、容易に復号化することができるので、少ない労力で秘密を保持することができる。

【0029】請求項8記載の発明は、請求項6記載のデータ通信装置において、前記復号化指示データ記憶手段は、前記データを復号化するキーワードを記憶しており、前記復号化手段は、この復号化指示データ記憶手段に記憶されているキーワードに基づいて前記データを復号化することを特徴とする構成とした。

【0030】請求項8記載の発明のデータ通信装置によれば、請求項6記載のデータ通信装置において、復号化指示データ記憶手段は、データを復号化するキーワードを記憶しており、復号化手段は、この復号化指示データ記憶手段に記憶されているキーワードに基づいて前記データを復号化する。

【0031】また、請求項9記載の発明は、請求項8記載のデータ通信装置において、前記復号化手段は、前記復号化指示データ記憶手段にキーワードが記憶されていると前記データを復号化することを特徴とする構成とした。

【0032】この請求項9記載の発明のデータ通信装置によれば、復号化手段は、復号化指示データ記憶手段にキーワードが記憶されているとデータを復号化する。

【0033】従って、請求項8記載のデータ通信装置によれば、受信するデータが暗号化されたデータか否かを、キーワードによって設定することができるので、例えば、ある特定のテーマに関するデータを指定すること等が可能であり、データ毎に設定する場合に比べて、簡単な操作によって、設定漏れ等のミスのない設定を行うことができる。さらに、この請求項8記載の発明は、請求項9記載のデータ通信装置のように、キーワードが復号化指示データ記憶手段に記憶されていることを検知することによって復号化を行う構成とすることにより、より容易に実現可能である。

【0034】請求項10記載の発明は、請求項8記載のデータ通信装置において、前記暗号化あるいは非暗号化されたデータと共にキーワードを受信し、前記復号化手段は、受信したキーワードが前記復号化指示データ記憶手段に記憶されていると前記データを復号化することを特徴とする構成とした。

【0035】この請求項10記載の発明のデータ通信装

置によれば、請求項8記載のデータ通信装置において、暗号化あるいは非暗号化されたデータと共にキーワードを受信し、復号化手段は、受信したキーワードが前記復号化指示データ記憶手段に記憶されていると前記データを復号化する。

【0036】従って、データ本文とともに送信されるキーワードを参照することによって、請求項8記載の発明によって得られる効果を、さらに容易に得ることができる。

10 【0037】請求項11記載の発明は、請求項6、7、8、9または10記載のデータ通信装置において、前記復号化指示データ記憶手段は、前記記憶されている復号化指示データ毎あるいはキーワード毎に異なる復号化キーあるいは異なる復号化方式を記憶し、前記復号化手段は、この復号化指示データ記憶手段に記憶された復号化キーあるいは復号化方式に基づいて復号化することを特徴とする構成とした。

【0038】請求項11記載の発明のデータ通信装置によれば、請求項6、7、8、9または10記載のデータ通信装置において、復号化指示データ記憶手段は、記憶されている復号化指示データ毎あるいはキーワード毎に異なる復号化キーあるいは異なる復号化方式を記憶し、復号化手段は、復号化指示データ記憶手段に記憶された復号化キーあるいは復号化方式に基づいて復号化をする。

【0039】従って、復号化指示データあるいはキーワードが異なるデータに対しては、復号化キーあるいは復号化方式が異なるので、他のデータに適用された復号化キーあるいは復号化方式を流用することが困難であり、より確実に秘密を保持することができる。

【0040】請求項12記載の発明は、通信手段を介して接続された外部の通信機器との間でデータ通信を行うデータ通信装置を利用したデータ通信方法において、データを送受信することができる外部の通信機器を送受信先として記憶し、これらの各送受信先が、該送受信先との間のデータ通信を秘密化すべき秘密通信先か否かをそれぞれ指定する秘密指定データを記憶し、この秘密指定データによって秘密通信先と指定された前記送受信先に対してデータを送信する際には、該データを暗号化して送信し、前記秘密指定データによって秘密通信先と指定された前記送受信先から送信されたデータを受信した際には、該データを秘密データとして記憶し、前記秘密指定データによって秘密通信先と指定されない前記送受信先から送信されたデータを受信した際には、該データを通常データとして記憶すること、を特徴としている。

【0041】この請求項12記載の発明のデータ通信方法によれば、通信手段を介して接続された外部の通信機器との間でデータ通信を行うデータ通信装置を利用したデータ通信方法において、データを送受信することができる外部の通信機器を送受信先として記憶し、これらの

各送受信先が、該送受信先との間のデータ通信を秘密化すべき秘密通信先か否かをそれぞれ指定する秘密指定データを記憶し、この秘密指定データによって秘密通信先と指定された送受信先に対してデータを送信する際には、該データを暗号化して送信し、秘密指定データによって秘密通信先と指定された送受信先から送信されたデータを受信した際には、該データを秘密データとして記憶し、秘密指定データによって秘密通信先と指定されない送受信先から送信されたデータを受信した際には、該データを通常データとして記憶する。

【0042】従って、例えばアドレス帳機能を有するデータベースに記憶された各宛先に対して、それぞれ暗号化したデータを送信するか、あるいは通常のデータを送信するかを予め設定しておくことによって、送信するデータを作成して通常通り送信しても、情報の秘匿が必要な相手へのデータについては、自動的にデータが暗号化される。これによって、毎回データ通信を行う毎にデータの暗号化等を設定する必要がなく、作業者の操作を減らすことが可能であり、さらに秘密を確実に保持することができる。

【0043】また、予め指定した送信元から送信されたデータを受信すると、そのデータが秘密を守るべきデータであると自動的に判断して、専用の記憶手段に記憶する。これによって、秘密保持が必要なデータを受信した後、誤って自由に閲覧可能な記憶手段に記憶してしまうことがないので、秘密を確実に保持することができる。さらに、通常のデータを記憶する記憶手段も備えているので、特に秘密保持の必要がないデータを閲覧する際の手間が増えることはない。

【0044】請求項13記載の発明は、通信手段を介して接続された外部の通信機器との間においてデータ通信を行うデータ通信装置を利用したデータ通信方法において、予め任意に設定される鍵情報を記憶し、前記データ通信機器によって送受信されるデータの内容に、前記鍵情報記憶手段に記憶された鍵情報が含まれているか否かを検知し、前記データ通信装置によって前記データを送信する際に、該データの内容に前記鍵情報が検知された場合には、該データを暗号化して送信し、前記データ通信装置が前記データを受信した際に、該データの内容に前記鍵情報が検知された場合には、該データを秘密データとして記憶し、前記データ通信装置が前記データを受信した際に、該データの内容に前記鍵情報が検知されない場合には、該データを通常データとして記憶すること、を特徴としている。

【0045】請求項13記載の発明のデータ通信方法によれば、通信手段を介して接続された外部の通信機器との間においてデータ通信を行うデータ通信装置を利用したデータ通信方法において、予め任意に設定される鍵情報を記憶し、データ通信機器によって送受信されるデータの内容に、鍵情報記憶手段に記憶された鍵情報が含ま

れているか否かを検知し、データ通信装置によってデータを送信する際に、該データの内容に鍵情報が検知された場合には、該データを暗号化して送信し、データ通信装置がデータを受信した際に、該データの内容に鍵情報が検知された場合には、該データを秘密データとして記憶し、データ通信装置がデータを受信した際に、該データの内容に鍵情報が検知されない場合には、該データを通常データとして記憶する。

- 【0046】従って、予め設定された鍵情報が内容に含まれるデータは、送信の際に暗号化されてから送信されるので、特定のテーマに関するデータのみを暗号化して、秘密を保持することができる。例えば、「金利」に関するデータには、通常「金利」の語が多数含まれる。そこで、鍵情報として「金利」を設定すれば、「金利」に関するデータはすべて暗号化され、秘密を保持することができ、さらにひとつひとつのデータを暗号化する場合に比べて、操作の減少により、作業効率が向上し、さらに、誤って暗号化しないで送信してしまうなどのミスを減らすことができる。
- 【0047】また、予め設定された鍵情報が内容に含まれるデータを受信した際には、該データは通常のデータとは異なる専用の記憶手段に記憶されるので、特定のテーマに関するデータは、他のデータと一緒に閲覧することができなくなり、秘密を保持することができる。これによって、秘密にすべきデータを、誤って誰でも閲覧可能な状態にしてしまうことがなく、確実に秘密を保持することができる。さらに、通常のデータを記憶する記憶手段を別途備えるので、秘密保持の必要のないデータを閲覧する際の操作が増えてしまうことがない。
- 【0048】請求項14記載の発明は、通信手段を介して接続された外部の通信機器との間でデータ通信を行うためのコンピュータが読み取り可能なプログラムを格納した記憶媒体であって、データを送信するためのプログラムコードと、データを送信することが可能な他のデータ通信装置を送信先と、該送信先との間のデータ通信を秘密化すべき秘密通信先か否かをそれぞれ指定する秘密指定データを記憶するためのプログラムコードと、この秘密指定データによって秘密通信先と指定された前記送信先に対して、データを送信する際に、該データを暗号化して送信するためのプログラムコードと、を格納したことを持てている。
- 【0049】この請求項14記載の発明の記憶媒体によれば、通信手段を介して接続された外部の通信機器との間でデータ通信を行うためのコンピュータが読み取り可能なプログラムを格納した記憶媒体であって、データを送信するためのプログラムコードと、データを送信することができる送信先である他のデータ通信装置と、これらの送信先との間のデータ通信を秘密化すべき秘密通信先か否かをそれぞれ指定する秘密指定データを記憶するためのプログラムコードと、この秘密指定データによっ

11

て秘密通信先と指定された送信先に対してデータを送信する際に、該データを暗号化して送信するためのプログラムコードと、を格納している。

【0050】従って、予め、例えばアドレス帳機能を有するデータベースに記憶された各宛先に対して、それぞれ暗号化したデータを送信するか、あるいは通常のデータを送信するかを設定しておくことによって、送信するデータを作成して通常通り送信しても、情報の秘匿が必要な相手へのデータについては、自動的にデータが暗号化される。これによって、毎回データ通信を行う毎にデータの暗号化等を設定する必要がなく、作業者の操作を減らすことが可能であり、さらに秘密を確実に保持することができる。

【0051】請求項15記載の発明は、通信手段を介して接続された外部の通信機器との間においてデータ通信を行うためのコンピュータが読み取り可能なプログラムを格納した記憶媒体であって、データを送受信するためのプログラムコードと、任意に設定される鍵情報を記憶するためのプログラムコードと、送受信されるデータの内容に、前記鍵情報記憶手段に記憶された鍵情報が含まれているか否かを検知するためのプログラムコードと、前記送受信手段によってデータを送信するあるいはデータを受信した際に、該データの題名に前記鍵情報が検知された場合には、該データを暗号化して送信するあるいは該データを暗号化して記憶するためのプログラムコードと、を格納したことを特徴としている。

【0052】この請求項15記載の発明の記憶媒体によれば、通信手段を介して接続された外部の通信機器との間において、データ通信を行うためのコンピュータが読み取り可能なプログラムを格納した記憶媒体であって、データを送受信するためのプログラムコードと、任意に設定される鍵情報を記憶するためのプログラムコードと、送受信されるデータの内容に、鍵情報記憶手段に記憶された鍵情報が含まれているか否かを検知するためのプログラムコードと、送受信手段によってデータを送信するあるいはデータを受信した際に、該データの内容に鍵情報が検知された場合には、該データを暗号化して送信するあるいは該データを暗号化して記憶するためのプログラムコードと、を格納している。

【0053】従って、予め設定された鍵情報が内容に含まれるデータは暗号化されてから送信されるので、特定のテーマに関するデータのみを暗号化して、秘密を保持することができる。また、操作の減少によって作業効率が向上するとともに、誤って暗号化しないで送信してしまうなどのミスを減らすことができる。また、該データは暗号化して記憶することができるので、これによって、秘密にすべきデータを、誤って誰でも閲覧可能な状態にしてしまうことがなく、確実に秘密を保持することができる。

【0054】請求項16記載の発明は、請求項15記載

12

の記憶媒体において、前記暗号化されたデータを受信すると秘密データとして記憶し、該暗号化されていないデータを受信すると通常データとして記憶するためのプログラムコードをさらに格納したことを特徴としている。

【0055】請求項16記載の発明の記憶媒体によれば、請求項15記載の記憶媒体において、暗号化されたデータを受信すると秘密データとして記憶し、該暗号化されていないデータを受信すると通常データとして記憶するためのプログラムコードを格納する。

10 【0056】従って、秘密を保持することが必要なデータを受信した際には、該データは通常のデータとは異なる専用の記憶手段に記憶されるので他のデータと一緒に閲覧することができなくなり、秘密を保持することができる。これによって、秘密にすべきデータを、誤って誰でも閲覧可能な状態にしてしまうことがなく、確実に秘密を保持することができる。さらに、通常のデータを記憶する記憶手段を別途備えるので、秘密保持の必要なないデータを閲覧する際の操作が増えてしまうことがない。

20 【0057】

【発明の実施の形態】以下、この発明の実施の形態について、図1～図9の図面を参照しながら説明する。

【0058】(第1の実施の形態)まず、本発明の第1の実施の形態としてのデータ通信システム1の構成について説明する。

【0059】図1は、データ通信システム1の構成の概略を示す図である。図2は、図1のデータ通信装置10の内部構成を示すブロック図である。図3は、図2のデータ記憶部17に格納されるアドレスデータの構成を示す模式図である。図4は、図1のデータ通信装置10による電子メール送信処理を示すフローチャートである。図5は、図1のデータ通信装置10による電子メール受信処理を示すフローチャートである。図6は、図1のデータ通信システム1のデータ通信装置10による電子メール復号化処理を示すフローチャートである。

【0060】これらの図に示すように、データ通信システム1は、通信回線網2、メールサーバー3、屋内変換器4、基地局5、携帯電話機6、データ通信装置7、10等により構成され、各データ通信装置7、10及びメールサーバー3の間でデータ通信を行うことができる。なお、データ通信装置7、10のほか、通信回線網2にはその他の通信端末装置を多数接続することが可能であるが、ここでは図示しない。

【0061】通信回線網2は、デジタル信号化されたデータを伝達することが可能なISDN(Integrated Services Digital Network)回線、PSTN(Public Switched Telephone Network)回線等の公衆回線や、独立して構築された専用回線網であっても良く、この通信回線網2には基地局5及び屋内変換器4が接続されている。

13

【0062】基地局5は、複数の携帯電話機6との間で無線通信によってデータを送受信することが可能であり、データ通信装置7はこの携帯電話機6及び基地局5を介して通信回線網2に接続されている。

【0063】一方、データ通信装置10は、通信回線網2に屋内交換機4を介して接続されており、同じく通信回線網2に接続されているメールサーバー3及びデータ通信装置7との間でデータ通信を行なうことが可能である。

【0064】メールサーバー3は、各データ通信装置7、10に対応して、メールボックスと呼ばれる記憶領域を内部に有し、各メールボックスに含まれるデータは、対応するデータ通信装置7、10によって接続した場合に閲覧可能である。

【0065】データ通信装置7、10から送信された全ての電子メールはメールサーバー3が受信し、該電子メールの宛先に対応するメールボックス内に該電子メールを格納する。また、該電子メールの宛先であるデータ通信装置7、10に対して、電子メールが届いたことを示す電子メール受信信号を送信する。従って、データ通信装置7、10から送信される電子メールは、メールサーバー3を介して所望の宛先に送信され、受信される。

【0066】ここで、データ通信装置7、10によって送信される電子メールの内、秘密を保持すべき電子メールは全て暗号化処理を施した上で送信され、その電子メールの復号化には、予めデータ通信装置7、10間に定められたパスワードを照合する必要がある。

【0067】統一して、データ通信装置7、10の構成について、データ通信装置10を例にとって説明する。

【0068】図2に示すように、データ通信装置10はCPU11、表示部12、入力部13、音声入出力部14、プログラム記憶部15、RAM16、データ記憶部17、RTC18、通信部19、バス20により構成され、各部はバス20に接続されている。

【0069】CPU(Central Processing Unit)11は、プログラム記憶部15内に格納されるプログラムを読み込んでRAM16内に設けられたメモリエリアに展開して実行し、各種データをデータ記憶部17から読み込んで、通信部19を介してメールサーバー3に対する電子メール送信処理、メールサーバー3から送信される電子メール受信処理を実行する。さらにプログラム記憶部15から読み込んだプログラム、及び、入力部13や音声入出力部14から入力される指示に従って、データの暗号化及びデータの復号化処理を実行する。

【0070】また、CPU11は、メールサーバー3との間で実行される電子メール送受信処理において、該電子メールの内容を表示するための表示情報を生成して表示部12に出力するとともに、RTC18から入力される時刻を示す信号を基準として、電子メールの送受信時刻を表示部12に表示させる。また、予め入力されたユ

14

ーザの希望により、表示部12に出力すべき内容を、同時に音声入出力部14に音声として出力させる。

【0071】そして、通信部19によってメールサーバー3からの電子メール受信信号が受信されると、メールサーバー3に接続し、メールサーバー3内のメールボックス内に格納されている電子メールを読み込み、電子メール受信処理を実行する。

【0072】そして、電子メールの送受信処理において、電子メールの宛先あるいは送信元がデータ記憶部17内に格納された後述するアドレスデータに記載され、さらにシークレット登録されているか否かを判断し、シークレット登録されている場合には、電子メールの暗号化及び復号化や、閲覧の際のパスワード照合等の秘密保持の為のプログラムをプログラム記憶部15から読み込んで実行する。

【0073】表示部12は、CRT(Cathode Ray Tube)やLCD(Liquid Crystal Display)等により構成され、入力部12によって入力された電子メールの宛先や、CPU11がメールサーバー3に対して送信した電子メールの内容等について、CPU11から入力される表示情報に基づいて表示画面上に表示を実行する。

【0074】入力部13は、カーソルキー、数字入力キーおよび各種機能キーを備えたキーボード等によってなり、宛先の電話番号や電子メールのアドレス等のデータを入力する場合等に押下されたキーの押下信号をCPU11に出力する。また、必要に応じてマウス等のポインティングデバイス(Pointing Device)を備えても良い。

【0075】音声入出力部14は、マイク、スピーカー等の音声入力装置及び音声出力装置を備え、ユーザーが希望に応じて設定することにより、CPU11から入力される情報に基づいて、表示部12によって表示される宛先のアドレスや受信した電子メールの内容を音声によって出力する。また、音声によって入力されたデータ等をCPU11に出力して、例えば電子メール中に音声メッセージを挿入することが可能である。

【0076】プログラム記憶部15は、各種プログラムが記憶される記憶媒体を有し、この記憶媒体は磁気的、光学的記録媒体、若しくは半導体メモリで構成されている。この記憶媒体はプログラム記憶装置15に固定的に設けたもの、若しくは着脱自在に装着するものであり、この記憶媒体には、電子メール受信処理、蓄積されている電子メールの管理、電子メールの暗号化処理及び復号化処理等の処理をCPU11に実行させるためのプログラムが格納される。

【0077】また、上記のプログラム記憶部15が有する記憶媒体に記憶されるプログラムは、通信回線等を介して接続された他の機器から受信して記憶する構成にしてもよく、さらに、通信回線等を介して接続された他の機器側に上記記憶媒体を備えた記憶装置を設け、この記

10

20

30

40

50

15

憶媒体に記憶されているプログラムを通信回線を介して使用する構成としても良い。

【0078】R.A.M (Random Access Memory) 16は、CPUにより処理される各種プログラムや、その処理に係るデータを一時的に格納するメモリエリアを形成する。

【0079】データ記憶部17は、データ通信装置10によって電子メールを送信する宛先や、データ通信装置10に対して電子メールを送信する送信元の電話番号やアドレスをアドレスデータとして記録し、各宛先及び送信元との間のデータ通信において秘密保持が必要か否かを示す情報とともに記憶する記憶媒体を備えている。この記憶媒体には、受信した電子メールや、ユーザが作成した電子メールを格納する記憶領域が設けられ、データ記憶部17は、CPU11から入力される読み出し信号に従って、各データをCPU11に出力する。

【0080】また、データ記憶部17が有する記憶媒体内に設けられた電子メールの記憶領域は、シークレットボックスと、通常メールボックスとに分割されている。

【0081】ここで、シークレットボックスとは、後述する秘密保持のための手段が適用されるシークレット登録データを格納する記憶領域であり、格納されたデータ内容を閲覧するためにはパスワード入力等の処理が必要である。一方、通常メールボックスは、通常の電子メールを格納する記憶領域であり、格納されたデータは容易に閲覧可能である。

【0082】RTC (Real Time Clock) 18は、内部に備えた水晶発振器等を基準として計時を行い、随時、日付及び時刻を示す情報をCPU11に出力する。

【0083】通信部19は、通信回線網2に接続され、変調回路、復調回路、送・受信ミキサ等によって構成され、CPU11から入力される指示に従って、通信回線網2を介して電子メールの送受信を実行し、また、メールサーバー3から通信回線網2を介して送信される電子メール受信信号を受信すると、該電子メール受信信号をCPU11に出力し、CPU11から電子メールの読み込みが指示されると、メールサーバー3に接続して電子メールを受信し、該電子メールの内容をCPU11に出力する。

【0084】図3には、図2のデータ記憶部17に格納されるアドレスデータの構成を示す。このアドレスデータにおいては、各宛先に対応する電子メールアドレスと宛先の氏名が記載される。例えば、図3の欄D1に記載されたアドレスは、「佐藤博司」という人物のメールアドレスである。

【0085】さらに、各メールアドレスに対応して、フラグの状態が記載されている。このフラグは、各宛先との間でデータ通信を実行する場合に、その通信内容の秘密の保持を指定するシークレット登録の有無を指定するもので、このフラグが「ON」に設定されている場合に

16

は、該宛先はシークレット登録され、この宛先との間でやりとりされるデータはシークレット登録データとして扱われ、後述する電子メールの暗号化処理等の秘密保持のための処理が適用される。一方、フラグが「OFF」の場合には、その宛先がシークレット登録されていないことを示し、その宛先との間では通常の電子メールの送受信等が行われる。

【0086】例えば、図3のD1に記載されたアドレスは「佐藤博司」という個人のアドレスである。このアドレスに対して送信されるデータは個人的なものであり、データが他者に漏洩することを避けるため、フラグは「ON」に設定され、このアドレスはシークレット登録されている。一方、図3のD3に記載されたアドレスは「江戸大学」のメールアドレスである。大学との間でやりとりされるデータには、一般的に公開される性質のデータが多く、全てのデータを秘密にする必要がないという理由から、シークレット登録されていない。

【0087】続いて、データ通信装置10の動作について説明する。

【0088】図4は、電子メールの送信時における暗号化処理を示すフローチャートである。データを送信する場合には、まず、ステップS1において、図3に示すアドレスデータを参照し、送信する電子メールの宛先がシークレット登録されているか否かを調べ、ステップS2に移行する。

【0089】ステップS2において、フラグが「ON」である、この電子メールはシークレット登録データであると判断された場合には、ステップS3に移行して、電子メールの内容を暗号化し、ステップS4に移行する。

【0090】また、ステップS2において、シークレット登録データではないと判断された場合には、ステップS4に移行する。

【0091】ステップS4では、電子メールを通信部19からメールサーバー3に対して送信し、電子メール送信処理を終了する。

【0092】次に、図5に従って、データ通信装置10による電子メール受信に係る一連の処理について説明する。

【0093】ステップS11では、メールサーバー3から送信された電子メール受信信号を受信し、メールサーバー3内のメールボックスから電子メールを読み込んで受信する。続いてステップS12において、受信した電子メールを送信した送信元を確認し、データ記憶部17内のアドレスデータと照合して、ステップS13に移行する。

【0094】ステップS13では、受信した電子メールの送信者がシークレット登録されているか、そうでないかを判断する。このステップS13において、シークレット登録データであると判断された場合には、ステップS14に移行して、受信した電子メールをシークレット

50

17

ポックスに蓄積して処理を終了する。

【0094】また、ステップS13において、該電子メールを送信した送信元がデータ記憶部17のアドレスデータに記載されていない、あるいはシークレット登録されていないと判断された場合には、ステップS15に移行して、受信した電子メールを通常メールボックス内に蓄積する。受信した電子メールの蓄積が終了すると、電子メール受信処理を終了する。

【0095】上記のように受信され、通常メールボックスに蓄積された電子メールは容易に閲覧可能であるが、シークレットボックス内に蓄積された電子メールを閲覧するためには、図6に示す処理が必要である。

【0096】ステップS21においては、シークレットボックス内に蓄積された電子メールのうち、閲覧したい電子メールが指定され、ステップS22に移行する。ステップS22では、パスワードの入力がなされ、続くステップS23でパスワードの照会が行われる。

【0097】シークレットボックスに蓄積された電子メールは、秘密の保持が必要な電子メールであり、その内容は暗号化されている。このため、そのままの状態で閲覧しても内容を理解することができない。そこで復号化を試みることになるが、復号化の際には、予め送信元との間で定められたパスワードを入力する必要がある。

【0098】ステップS23では、ステップS22で入力されたパスワードが、予め送信相手と設定されたパスワードと一致するか否かを判定し、一致しない場合にはステップS26に移行して、表示部12にエラーメッセージを表示し、処理を終了する。

【0099】また、ステップS23においてパスワードが一致した場合には、ステップS24に移行する。ステップS24では、指定された電子メールを復号化し、ステップS25に移行して該電子メールを表示部12に表示して、処理を終了する。

【0100】以上のように、この第1の実施の形態によれば、秘密を保持する必要がある相手に対する電子メールの送受信処理においては、予め宛先と秘密保持の必要な有無をアドレスデータに記載してシークレット登録しておくことによって、電子メールを送信する際には該電子メールが自動的に暗号化され、電子メールを受信する際には、シークレットボックス内に蓄積される。そして、このシークレットボックス内に蓄積された電子メールは暗号化されており、正しいパスワードを入力することによって閲覧することが可能であるので、データ通信装置10を他人が使用している場合であっても、容易に秘密を保持することが可能である。また、シークレット登録していない宛先との間の電子メールの送受信は通常通り実行されるため、必要以上に秘密保持の処理が行われることはなく、煩雑な処理を強いられることがない。

【0101】なお、上記第1の実施の形態においては、シークレット登録された宛先から送信された電子メール

18

は暗号化されているものとしたが、暗号化されていない電子メールをシークレットボックス内に蓄積することも勿論可能である。なお、この場合には、秘密の保持のために、シークレットボックスを閲覧するためのパスワードを設定しておき、このパスワードの照合によってシークレットボックス内の電子メールを閲覧するものとしても良い。また、シークレットボックス内の電子メールを復号化するためのパスワードは、予め送信元との間で定めておくものとしたが、メールサーバー3とデータ通信装置10との間で定めることとしても良い。

【0102】(第2の実施の形態) 次に、本発明の第2の実施の形態としてのデータ通信システムについて説明する。なお、第2の実施の形態であるデータ通信システムの構成は、上記第1の実施の形態であるデータ通信システム1と共通であるので、図7に動作を示すフローチャートを示し、構成についての図示及び説明は省略する。

【0103】このデータ通信システム1におけるデータ通信装置10は、データ記憶部17に格納されたアドレスデータ内に、各宛先との間で定められた、電子メール復号化の為のパスワードを記憶する。CPU11は、このパスワードを読み込むことによって、パスワードを入力し、暗号化された電子メールを復号化する。

【0104】図7は、電子メール受信に係る一連の処理を示すフローチャートである。

【0105】ステップS31では、メールサーバー3から送信された電子メール受信信号を通信部19において受信し、メールサーバー3に接続して該電子メールを読み込んで受信する。

【0106】続いて、ステップS32では、該電子メールを送信した送信元を確認するとともに、データ記憶部17内のアドレスデータと照合し、ステップS33に移行する。ステップS33では、受信した電子メールの送信者がシークレット登録されているか、そうでないかを判断する。

【0107】ステップS33において、該電子メールを送信した送信元がデータ記憶部17のアドレスデータに記載されていない、あるいはシークレット登録されていないと判断された場合には、ステップS38に移行して、受信した電子メールを通常メールボックス内に蓄積し、処理を終了する。

【0108】また、ステップS33において、受信した電子メールの送信元がシークレット登録されていると判断された場合には、ステップS34に移行する。

【0109】ステップS34では、電子メールを送信した送信元に対応するパスワードを、データ記憶部17内のアドレスデータから読み込み、照合を行う。即ち、アドレスデータに記載されたパスワードが誤りであった場合には、復号化処理を行っても拒否されてしまい、復号化は失敗する。

19

【0110】ステップS35でパスワードが一致せずに、復号化に失敗した場合にはステップS37に移行して、復号化を行わずに電子メールをシークレットボックス内に蓄積して、処理を終了する。

【0111】ステップS35でパスワードが一致した場合には、ステップS36に移行して電子メールの復号化を実行し、ステップS37で復号化されたデータをシークレットボックス内に蓄積し、処理を終了する。

【0112】以上のように、この第2の実施の形態によれば、予め各宛先との間で設定されたパスワードを各宛先に対応してアドレスデータ内に記載し、電子メールを受信した際にこのパスワードを読み込むことによって、電子メールの受信と同時に復号化を行うことが可能であり、シークレットボックス内に蓄積されたデータであってもすばやく閲覧することができる。また、パスワードが一致しない場合には復号化は不可能であるが、暗号化されたままの電子メールはシークレットボックスに蓄積されるので、改めてパスワードを確認した後に電子メールを復号化することによって閲覧することができる。

【0113】(第3の実施の形態)図8及び図9は本発明の第3の実施の形態としてのデータ通信システムの動作を示すフローチャートである。なお、第3の実施の形態であるデータ通信システムの構成は、上記第1の実施の形態であるデータ通信システム1と共に用意されるので、図8及び図9に動作を示すフローチャートを示し、構成についての図示及び説明は省略する。

【0114】この第3の実施の形態であるデータ通信システム1におけるデータ通信装置10は、データ記憶部17内に、予めキーワードが入力され、記憶されている。このキーワードは、ある特定のテーマに関する電子メールの秘密の保持を目的とし、秘密にしたい電子メールのテーマを示すようなキーワードが設定される。

【0115】図8は、電子メールの送信に係る一連の処理を示すフローチャートである。

【0116】ステップS40においては、メールサーバー3に対して電子メールを送信する際に、その電子メールの内容と、データ記憶部17内に格納されたキーワードを照合する。内容にキーワードが含まれている場合には、秘密にしたいテーマに沿った内容が記載された電子メールであると判断する。

【0117】ステップS41において、送信する電子メールの内容のキーワードの検出を実行する。このステップS41で、キーワードが検出された場合には、この電子メールは秘密保持の為の処理を適用すべきであると判断して、ステップS42へ移行する。

【0118】ステップS42では暗号化処理を行うと共に、キーワードをヘッダ情報に付加し、ステップS43に移行して、メールサーバー3に対して、該ヘッダ情報と共に該メールを送信する。

【0119】ステップS41で、電子メールの内容にキ

20

ーワードが検出されない場合には、ステップS43へ移行して、この電子メールを送信し、処理を終了する。

【0120】図9は電子メールの受信に際して、暗号化された電子メールの受信に係る一連の処理を示すフローチャートである。なお、受信した電子メールのうち、暗号化されていない電子メールに関しては通常の処理を行うので説明を省略する。

【0121】ステップS45では、メールサーバー3から電子メールを受信し、受信した電子メールが暗号化されていた場合には、ステップS46に移行する。

【0122】ステップS46では、受信した電子メールのヘッダ情報の内容と、データ記憶部17に格納されたキーワードを照合する。

【0123】ステップS47で、電子メールのヘッダ情報の内容にキーワードが検出された場合にはステップS48に移行し、キーワードに対応する復号化処理によって電子メールの復号化を実行し、受信した電子メールの内容にキーワードが検出されなかった場合には、ステップS49に移行する。

【0124】ステップS48では、暗号化されている電子メールの復号化を行い、ステップS49に移行する。

【0125】ステップS49では、電子メールをメールボックス内に蓄積して処理を終了する。

【0126】なお、上記第3の実施の形態において、暗号化に際しては、複数の暗号化方式を用意し、復号化に際しては複数の復号化方式を予め用意して、異なるキーワードに対して異なる方式を適用する構成とすれば、より確実な秘密保持が可能である。

【0127】具体的には、予め、データ記憶部17内に、キーワードと共に、各キーワードに適用される暗号化方式及び復号化方式を指定する。また、プログラム記憶部15内には、各々異なる方式によって暗号化及び復号化を行う暗号化プログラム、復号化プログラムを複数格納し、CPU11は、データ記憶部17内のデータによって指定された暗号化プログラム及び復号化プログラムを読み込んで実行する。

【0128】図8のステップS40において、送信する電子メールの内容においてキーワードの検出を行い、ステップS41においてキーワードが検出された場合には、ステップS42に移行し、該キーワードに対応する暗号化プログラムによって暗号化を行う。

【0129】また、図9のステップS45において暗号化された電子メールを受信した場合には、ステップS46において、該電子メールのヘッダ部とデータ記憶部17内に格納された複数のキーワードを照合する。

【0130】ステップS47でキーワードが検出された場合には、ステップS48において、プログラム記憶部15内に格納された複数の復号化プログラムの中から、該キーワードに対応するよう設定されたプログラムによって復号化を行う。その後、ステップS49で、復号化

50

21

された電子メールをメールボックス内に蓄積し、処理を終了する。

【0131】また、暗号化及び復号化の際には、暗号化キー及び復号化キーと呼ばれるパスワードが設定されることがある。この暗号化キー及び復号化キーを、データ記憶部17内に、複数のキーワードに対応づけて格納する構成とすることも可能である。

【0132】即ち、図8のステップS41においてキーワードを検出した際に、該キーワードに対応する暗号化キーをデータ記憶部17から読み込み、ステップS42で、この暗号化キーを用いて暗号化を実行する。

【0133】また、図9のステップS47においてキーワードが検出された場合には、該キーワードに対応する復号化キーをデータ記憶部17から読み込んで、ステップS48で復号化を行う構成とすればよい。

【0134】以上のように、この第3の実施の形態によれば、電子メールの宛先及び送信元を問わず、電子メールに付された内容にキーワードが含まれる場合に、秘密保持が必要と判断する。このため、秘密を保持したいテーマについての電子メールであれば、どの宛先及び送信元との電子メールのやりとりにおいても漏れがなく、確実に秘密を保持することができる。また、各宛先毎の設定が不要であるので、容易に、特定のテーマに関して秘密保持ができる。

【0135】なお、暗号化した電子メールに対してヘッダ情報にキーワードを附加したが、本発明はこれに限定されることはなく、ヘッダ情報にキーワードを附加することなく電子メールを送信し、受信側でキーワードに関係なく、予め設定されたパスワードに基づいて復号化を行う構成としても良い。

【0136】なお、上記実施の形態においては、データ通信装置7、10を通信回線網2に接続された構成としたが、LAN (Local Area Network) を構築して各データ通信装置を接続した構成としても良いし、また、異なるネットワークに接続されたデータ通信装置間において、インターネット (The Internet) 等を介して電子メールを送受信する構成としたが、直接データ通信装置間において電子メールを送受信する構成としても良いし、その他、細部の構成についても、本発明の趣旨を逸脱しない範囲で、任意に変更可能であることは勿論である。

【0137】

【発明の効果】請求項1記載の発明によれば、予め暗号化指示データ記憶手段によって暗号化すべきデータを指定しておくことによって、データを送信する毎にデータの暗号化を指示する必要がなく、作業者の操作を減らすことが可能であり、さらに秘密を確実に保持することができる。

【0138】請求項2記載の発明によれば、例えばアド

22

レス帳機能を有するデータベースに記載された各宛先に対して、それぞれ暗号化したデータを送信するか、あるいは通常のデータを送信するかを予め設定しておくことによって、データを通常通り送信しても、情報の秘匿が必要な相手へデータを送信する場合には、自動的にデータが暗号化される。

【0139】請求項3記載の発明によれば、予め設定されたキーワードを含むデータの暗号化が実行されるので、ある特定のテーマに関するデータを全て暗号化した

10 場合などに、各データ毎に暗号化を設定しなくても、該テーマをキーワードに設定することによって暗号化を行なうことができる。そして、各データについて設定を個々に行なう場合に比べて、設定漏れ等のミスを減少させることができる。

【0140】請求項4記載の発明によれば、請求項3記載の発明においてデータを送信する際に、例えば、電子メールのタイトルのような形式によってキーワードがデータ本文に付されて送信されるので、データ本文を参照することなくキーワードを容易に認識することが可能と

20 なり、利便性をより高めることができる。

【0141】請求項5記載の発明によれば、暗号化指示データあるいはキーワードが異なるデータに対しては、暗号化キーあるいは暗号化方式が異なるので、他のデータに適用された暗号化キーあるいは暗号化方式を容易に流用することが困難になるので、より確実に秘密を保持することができる。

【0142】請求項6記載の発明によれば、データ通信装置において受信したデータが暗号化されているか否かを予め設定することが可能であるので、暗号化されたデータを受信するとともに該データを復号化することができる。従って、データを受信して閲覧する毎に復号化を

30 設定する必要がなく、作業者の操作を減らすことが可能である。

【0143】請求項7記載の発明によれば、秘密を保持したいデータを送受信する相手先を予め登録しておくことによって、容易に復号化することができるので、少ない労力で秘密を保持することができる。

【0144】請求項8記載の発明によれば、受信するデータが暗号化されたデータか否かを、キーワードによって設定することができるので、例えば、ある特定のテーマに関するデータを指定すること等が可能であり、データ毎に設定する場合に比べて、簡単な操作によって、設定漏れ等のミスのない設定を行うことができる。

【0145】請求項9記載の発明によれば、請求項8記載の発明において、キーワードが復号化指示データ記憶手段に記憶されていることを検知することによって復号化を行う構成とすることにより、より容易に実現可能と/orすることができる。

【0146】請求項10記載の発明によれば、データ本文とともに送信されるキーワードを参照することによっ

50

て、請求項8記載の発明によって得られる効果を、さらに容易に得ることができる。

【0147】請求項11記載の発明によれば、復号化指示データあるいはキーワードが異なるデータに対しては、暗号化キーあるいは復号化方式が異なるので、他のデータに適用された復号化キーあるいは復号化方式を適用することが困難であるので、より確実に秘密を保持することができる。

【0148】請求項12記載のデータ通信方法によれば、例えばアドレス帳機能を有するデータベースに記憶された各宛先に対して、それぞれ暗号化したデータを送信するか、あるいは通常のデータを送信するかを予め設定しておくことによって、送信するデータを作成して通常通り送信しても、情報の秘匿が必要な相手へのデータについては、自動的にデータが暗号化される。これによって、毎回データ通信を行う毎にデータの暗号化等を設定する必要がなく、作業者の操作を減らすことが可能であり、さらに秘密を確実に保持することができる。

【0149】また、予め指定した送信元から送信されたデータを受信すると、そのデータが秘密を守るべきデータであると自動的に判断して、専用の記憶手段に記憶する。これによって、秘密保持が必要なデータを受信した後、誤って自由に閲覧可能な記憶手段に記憶してしまうことがないので、秘密を確実に保持することができる。さらに、通常のデータを記憶する記憶手段も備えているので、特に秘密保持の必要がないデータを閲覧する際の手間が増えることはない。

【0150】請求項13記載のデータ通信方法によれば、予め設定された鍵情報が内容に含まれるデータは、送信の際に暗号化されてから送信されるので、特定のテーマに関するデータのみを暗号化して、秘密を保持することができる。さらに、ひとつひとつのデータを暗号化する場合に比べて、操作の減少によって作業効率が向上し、また、誤って暗号化しないで送信してしまうなどのミスを減らすことができる。

【0151】そして、予め設定された鍵情報が内容に含まれるデータを受信した際には、該データは通常のデータとは異なる専用の記憶手段に記憶されるので、特定のテーマに関するデータは、他のデータと一緒に閲覧することができなくなり、秘密を保持することができる。これによって、秘密にすべきデータを、誤って誰でも閲覧可能な状態にしてしまうことがなく、確実に秘密を保持することができる。さらに、通常のデータを記憶する記憶手段を別途備えるので、秘密保持の必要なデータを閲覧する際の操作が増えてしまうことがない。

【0152】請求項14記載の記憶媒体によれば、予め、例えばアドレス帳機能を有するデータベースに記憶された各宛先に対して、それぞれ暗号化したデータを送信するか、あるいは通常のデータを送信するかを設定しておくことによって、送信するデータを作成して通常通

り送信しても、情報の秘匿が必要な相手へのデータについては、自動的にデータが暗号化される。これによって、毎回データ通信を行う毎にデータの暗号化等を設定する必要がなく、作業者の操作を減らすことが可能であり、さらに秘密を確実に保持することができる。

【0153】請求項15記載の記憶媒体によれば、従つて、予め設定された鍵情報が内容に含まれるデータは暗号化されてから送信されるので、特定のテーマに関するデータのみを暗号化して、秘密を保持することができる。また、操作の減少によって作業効率が向上するとともに、誤って暗号化しないで送信してしまうなどのミスを減らすことができる。また、該データは暗号化して記憶することができるので、これによって、秘密にすべきデータを、誤って誰でも閲覧可能な状態にしてしまうことがなく、確実に秘密を保持することができる。

【0154】請求項16記載の記憶媒体によれば、秘密を保持する必要があるデータを受信した際には、該データは通常のデータとは異なる専用の記憶手段に記憶されるので他のデータと一緒に閲覧することができなくなり、秘密を保持することができる。これによって、秘密にすべきデータを、誤って誰でも閲覧可能な状態にしてしまうことがなく、確実に秘密を保持することができる。さらに、通常のデータを記憶する記憶手段を別途備えるので、秘密保持の必要なデータを閲覧する際の操作が増えてしまうことがない。

#### 【図面の簡単な説明】

【図1】本発明の第1の実施の形態としてのデータ通信システムの構成を示す概略図である。

【図2】図1のデータ通信装置の内部構成を示すブロック図である。

【図3】図2のデータ記憶部に格納されるアドレスデータの構成を示す図である。

【図4】図1のデータ通信システムによる電子メール送信処理を示すフローチャートである。

【図5】図1のデータ通信システムによる電子メール受信処理を示すフローチャートである。

【図6】図1のデータ通信システムによる電子メール復号化処理を示すフローチャートである。

【図7】本発明の第2の実施の形態としてのデータ通信システムによる電子メール受信処理を示すフローチャートである。

【図8】本発明の第3の実施の形態としてのデータ通信システムによる電子メール送信処理を示すフローチャートである。

【図9】図8のデータ通信システムによる電子メール受信処理を示すフローチャートである。

#### 【符号の説明】

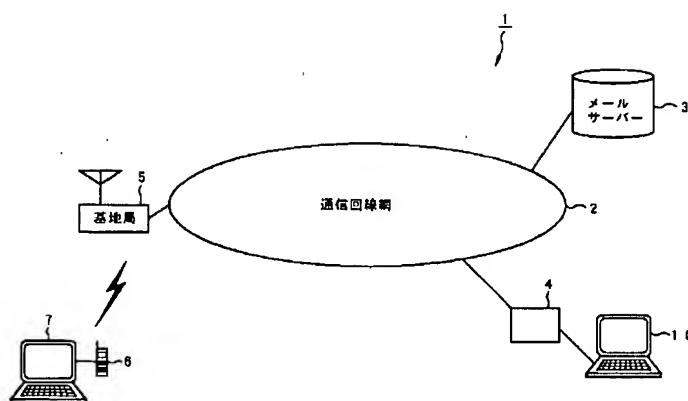
- |   |           |
|---|-----------|
| 1 | データ通信システム |
| 2 | 通信回線網     |
| 3 | メールサーバー   |

25

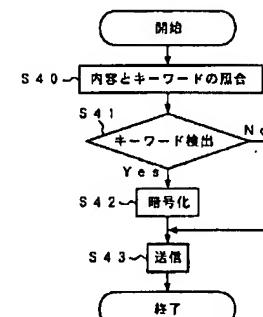
- 4 屋内変換器  
 5 基地局  
 6 携帯電話機  
 7, 10 データ通信装置  
 11 CPU  
 12 表示部  
 13 入力部

- 14 音声入出力部  
 15 プログラム記憶部  
 16 RAM  
 17 データ記憶部  
 18 RTC  
 19 通信部  
 20 バス

【図1】



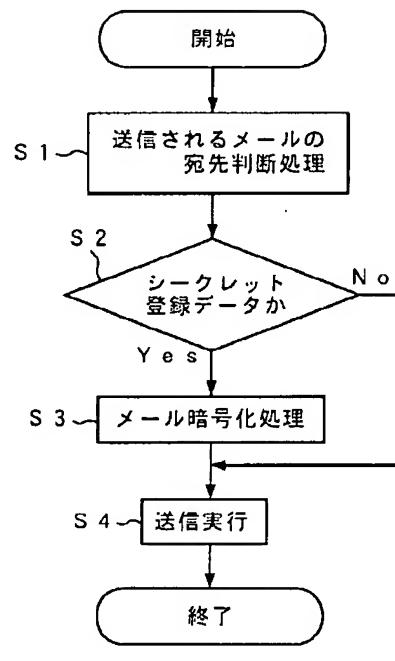
【図8】



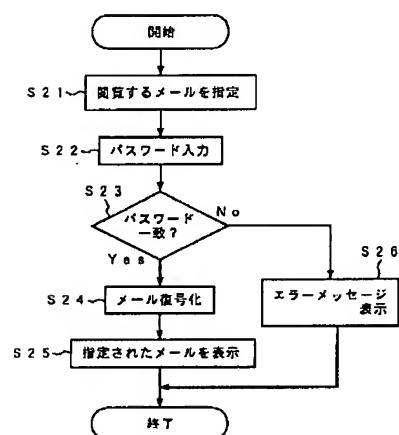
【図3】

|    | アドレス                     | 氏名    | フラグ   |
|----|--------------------------|-------|-------|
| D1 | a@caslow.rd.sato.or.jp   | 佐藤博司  | ON    |
| D2 | b@caslow.rd.yamada.co.jp | 山田亮介  | ON    |
| D3 | c@caslow.rd.edo-u.ac.jp  | 江戸大学  | OFF   |
|    | .....                    | ..... | ..... |

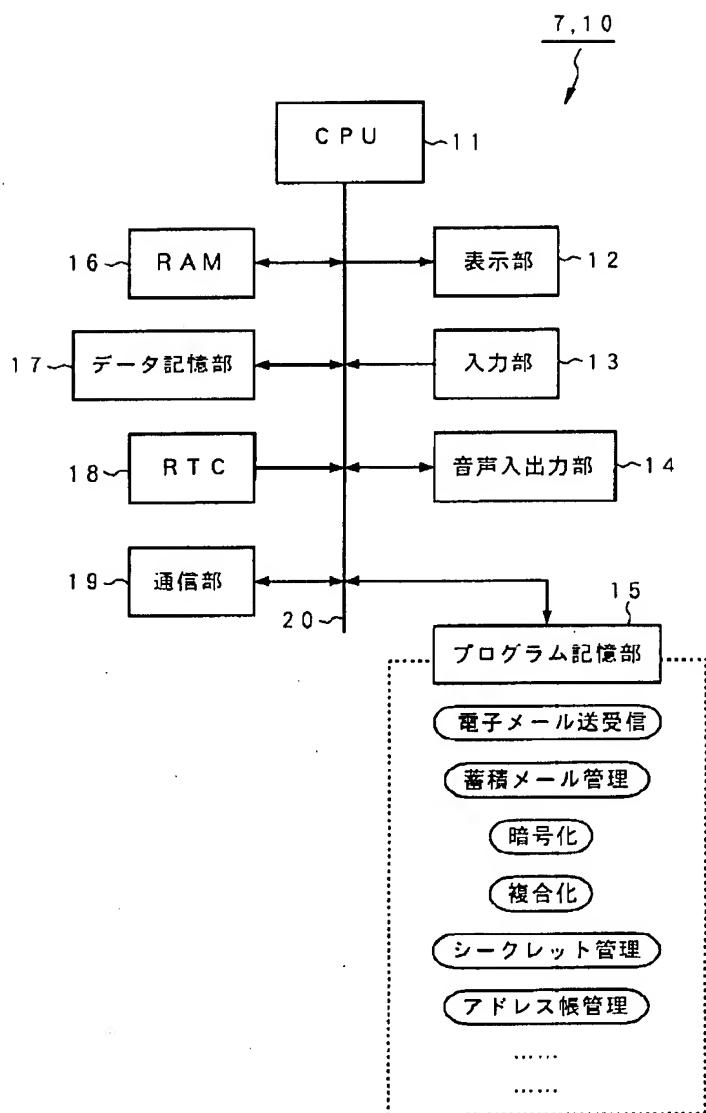
【図4】



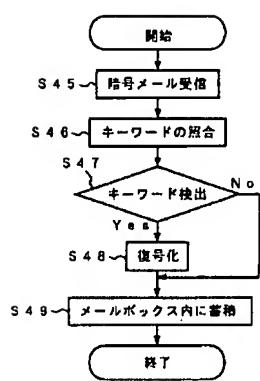
【図6】



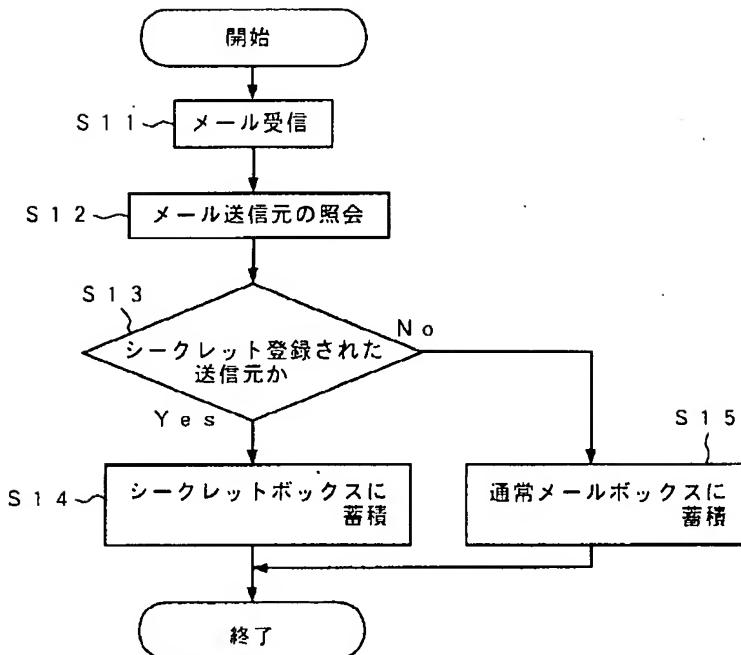
【図2】



【図9】



【図5】



【図7】

